GUIDE D'INVESTISSEMENT

Cybersécurité, la Grande Menace

Les actions incontournables pour profiter de l'essor de l'industrie de la protection informatique



Par les experts de

zonebourse


SHOUT
SHARE
IT

Sommaire

L'Avènement du Numérique 5

Aux sources du crime 6

Un terreau favorable renforcé par plusieurs facteurs 7

À qui profite le crime ? 9

Les Moyens et les Enjeux 14

Les menaces qui pèsent sur une entreprise 15

Barbarians at the gate 18

Notre Sélection de Valeurs 25

Édito



Franck Morel
Président Fondateur de Zonebourse.com

Après le succès de notre premier dossier consacré à l'industrie du Cannabis, je suis heureux de vous proposer une seconde étude sur la Cybersécurité.

Les décryptages Zonebourse identifient et analysent des thématiques d'investissement porteuses à long terme, pour vous aider à profiter des meilleures opportunités dans les secteurs d'avenir grâce aux puissants outils Surperformance.

Bonne lecture à tous.

Franck Morel



Anthony Bondain
Rédacteur en chef Zonebourse.com

Projetez-vous en 2027. Le soleil n'est pas tout à fait levé, vous attendez devant chez vous, avec famille et bagages, le taxi qui doit vous emmener à l'aéroport pour partir en vacances.

Quel degré de confiance dans la technologie vous faudra-t-il pour grimper dans le véhicule sans chauffeur qui vient de s'arrêter ?

Autre scénario. En 2022, votre petite entreprise réalisera près de la moitié de son chiffre d'affaires grâce à son site internet.
Comment faire pour assurer la sécurité de l'activité ? Et dès à présent, qu'est-ce qui garantit que vos données personnelles sont suffisamment protégées alors que vous les utilisez largement sur le web en faisant confiance à des tiers ?

Dans tous ces cas et bien d'autres, une partie de la solution passe par la cybersécurité.

Le monde hyperconnecté dans lequel nous évoluerons, nous évoluons déjà devrais-je dire, ne fera qu'accentuer le poids économique de la sécurité informatique au sens large.

Les pages qui suivent vont vous permettre de comprendre les enjeux du secteur.

Anthony Bondain

Interrogez des administrateurs de grandes entreprises au sujet des cybermenaces. Vous constaterez que la cybersécurité est devenue le sujet de préoccupation numéro un.

Un dirigeant sait généralement répliquer à un concurrent, gérer des mutations sectorielles ou répondre à une crise sociale.

Mais il est souvent démuni contre les menaces numériques, qu'il a plus de mal à appréhender. Pourtant, l'actualité lui rappelle constamment que leurs conséquences peuvent être désastreuses.



L'explosion du marché de la cybersécurité n'est pas un mirage, les chiffres le prouvent. Les dépenses consacrées à la protection contre les attaques informatiques représentaient entre 3,5 et 4 milliards de dollars annuels dans le monde en 2004.

La plupart des entreprises ne disposaient alors que d'un antivirus et d'un firewall, un peu comme le particulier aujourd'hui. Pour l'année 2018, les estimations varient entre bureaux d'études, parfois fortement, mais toutes dépassent 100 milliards de dollars, soit un multiple de 25 en quinze ans.

A l'avenir, la progression ne sera pas aussi impressionnante, mais ce marché devrait continuer à croître à deux chiffres, soit l'un des compartiments les plus dynamiques de l'informatique. Le cabinet Global Market Insights a estimé, dans une étude récente, que le chiffre d'affaires généré par le secteur pourrait avoisiner les 300 milliards de dollars par an en 2024. Cette évaluation est sans doute à considérer comme une borne haute, mais elle illustre l'inévitable essor de la sécurité informatique.

NB : Nous avons autant que possible privilégié l'utilisation de vocabulaire français pour les différents termes techniques, mais nous donnons entre parenthèses leur traduction anglaise, il faut bien l'avouer beaucoup plus répandue. Pour plus de clarté, nous utilisons à plusieurs reprises le terme de "pirate" pour qualifier l'individu dont la technique lui permet de se retrouver volontairement en un lieu de l'infrastructure informatique où il n'a rien à faire, quelles que soient ses intentions (malveillantes, éthiques, ludiques…).

L'Avènement du Numérique



Aux sources du crime

La numérisation de l'économie, ou sa digitalisation pour utiliser un anglicisme plus répandu, a connu une formidable accélération au cours des deux dernières décennies avec la révolution Internet et les progrès technologiques qui en ont découlé.

C'est elle qui a permis l'avènement des Apple, Alphabet, Microsoft, Amazon ou Facebook, qui sont devenues les plus grosses entreprises du monde, reléguant les pans plus traditionnels de l'économie au second plan.

Mais ce phénomène va bien au-delà des entreprises du numérique : il est très difficile d'y échapper. Les lignes de production d'un équipementier automobile sont numérisées. Le système logistique d'un aciériste l'est aussi.

Même le matériel de certaines exploitations agricoles, une partie des échanges avec les services publics ou le système de vente à distance d'une créatrice de meubles pour enfants.
Toutes les entreprises et les administrations du monde utilisent des logiciels connectés au réseau. De la multinationale au boulanger du coin. Et des milliards de particuliers se connectent. Rien qu'en France, 94% de la population de plus de 12 ans dispose d'un téléphone mobile, et 86% d'une connexion internet.

La numérisation galopante crée des passerelles entre des systèmes qui ne se côtoyaient pas jusque-là. **L'accroissement de la capacité des réseaux et le développement des services dans le nuage ("cloud") y contribue fortement.**

Avec l'interconnexion mondiale, l'effet papillon n'est pas un vain mot. Dans un tel contexte, le pirate profite d'un terrain de jeu de plus en plus vaste et d'un avantage de poids sur ses contemporains : il ne se contente pas de profiter des services de la révolution numérique, il en maîtrise les rouages techniques, ou du moins une partie d'entre eux.



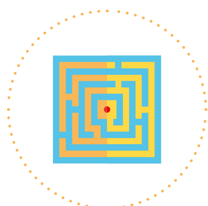
L'affrontement devient asymétrique : un individu isolé est capable de faire beaucoup de tort à une grande institution

Cet atout considérable lui permet d'avoir, souvent, un coup d'avance. Les machines sont protégées par des outils plus puissants quand elles sont en réseau ? Ce réseau permet d'attaquer davantage de machines en cas d'infection. Plus de 50% du trafic web mondial est chiffré pour améliorer la sécurité ?

Le chiffrement permet aux pirates de masquer leurs activités. Le cloud permet d'accélérer les mises à jour critiques pour éviter les attaques ? Il crée de nouvelles vulnérabilités. Les objets connectés se multiplient ? Ce sont autant de portes d'entrées supplémentaires dans les réseaux pour des individus mal intentionnés. La liste est longue.

Toute nouvelle connexion à un réseau est synonyme de nouvelle possibilité d'intrusion, comme le signale l'ANSSI, l'organisme français spécialisé dans la sécurité des systèmes d'information.

Un terreau favorable renforcé par plusieurs facteurs

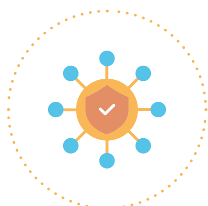


D'abord, **les barrières à l'entrée du monde informatique semblent relativement élevées**, ce qui crée auprès du grand public un sentiment de complexité et d'impuissance.



Ensuite, **les chaînes numériques sont de plus en plus longues**. Nous parlons ici de la somme des outils informatiques déployés entre l'utilisateur et le service.

Par exemple, entre un consommateur et un achat sur internet, interviennent des technologies publicitaires, web, d'identification, de paiement, de livraison, de satisfaction client etc.



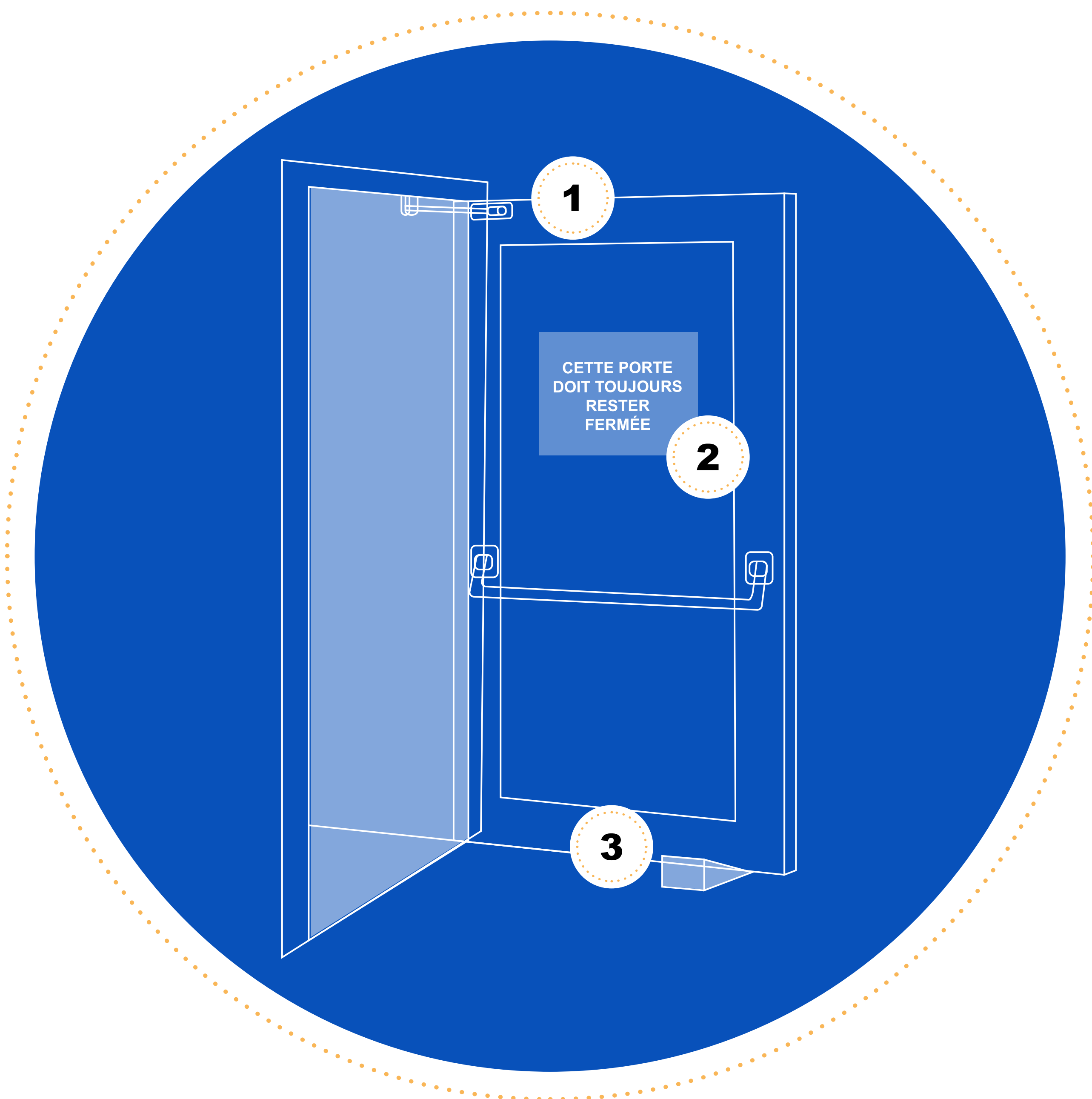
En outre, **l'affrontement devient asymétrique**, au sens où un individu isolé avec des moyens limités est capable de faire beaucoup de tort à une grande institution.

Le défenseur doit penser à toutes les interactions et doit souvent faire confiance à des applications tierces.



Enfin, **les usages modernes tendent à mêler vie numérique professionnelle et personnelle**, un vrai casse-tête pour les services informatiques d'une entreprise, confrontés à la prolifération de l'informatique de l'ombre ("shadow IT"), c'est-à-dire des matériels et des logiciels introduits par les utilisateurs sans avoir été autorisés.

Cette situation et plus généralement le télescopage entre les exigences de sécurité d'une organisation et la souplesse souhaitée par les utilisateurs trouve une excellente illustration utilisée dans une présentation Microsoft datant de plusieurs années (voir ci-dessous).



1 Le groom symbolise le système de sécurité mis en place par l'entreprise

2 Le panneau représente la consigne du service informatique

3 La cale, c'est le comportement utilisateur

A qui profite le (cyber)crime ?

Le terme générique de "pirate" ne fait pas l'unanimité. Selon Littré, le pirate est "celui qui n'a de commission d'aucun gouvernement, et qui court les mers pour piller".

Pour Larousse, c'est un "aventurier qui courait les mers pour piller des navires", une définition partagée par l'Académie, qui ajoute que cela se dit aussi, "par extension, de tout homme qui s'enrichit malhonnêtement et aux dépens d'autrui, qui commet des exactions criantes". Nous verrons dans les paragraphes qui suivent que **le pirate des temps modernes est souvent mû par l'appât du gain, mais qu'il sait aussi se faire militant, corsaire ou espion**.

Prenons un exemple très concret, qui nous accompagnera tout au long de notre dossier. En 2017, le monde fait la connaissance du virus baptisé NotPetya, qui a infecté plusieurs centaines de milliers d'ordinateurs dans le monde.

Ce rançongiciel ("ransomware") a été diffusé à partir de la mise à jour appliquée à un logiciel de comptabilité édité par une petite entreprise ukrainienne, largement utilisé par les sociétés locales. Très virulent, NotPetya s'est facilement frayé un chemin jusque dans les réseaux de certaines maisons-mères d'entreprises infectées, provoquant une panique mondiale. Des multinationales ont été paralysées.

L'opérateur de porte-conteneurs Maersk, qui a bien failli y laisser son système informatique, a évalué la facture à environ 300 millions de dollars (mais les bons connaisseurs du dossier savent qu'elle est encore plus lourde). **18 mois plus tard, en dépit de lourds soupçons pesant sur la Russie, personne ne connaît l'identité de l'attaquant ni son but**. Cette situation est récurrente et illustre la difficulté à parer les cybermenaces : leurs auteurs sont aussi multiples que leurs motivations sont nombreuses.



Il est de notoriété publique que certains outils prisés des pirates ont été développés par des entités liées de près ou de loin à des Etats

Lorsqu'un pays est impliqué, ses motivations sont géopolitiques ou économiques. Plusieurs groupes de hackers connus sont réputés être rattachés qui à la Chine, qui à la Russie, qui à la Corée du Nord, voire aux services secrets de puissances occidentales.

La plupart des Etats disposent désormais d'équipes de cybersécurité, à vocation défensive, offensive ou les deux, selon la doctrine militaire qu'ils ont adoptée.

Il est de notoriété publique que certains outils prisés des pirates ont été développés par des entités liées de près ou de loin à des Etats. NotPetya, encore lui, a d'ailleurs bénéficié du kit d'exploit EternalBlue volé par des hackers à la NSA américaine. Laquelle l'avait développé pour tirer parti d'une faille de sécurité de Microsoft, sans en révéler l'existence.

Pour caricaturer, les véritables cybercriminels sont en général motivés par l'appât du gain, les "hacktivistes" par l'idéologie etc. Le Centre canadien pour la cybersécurité, dans le tableau ci-contre, fournit quelques exemples d'auteurs et de motivations.



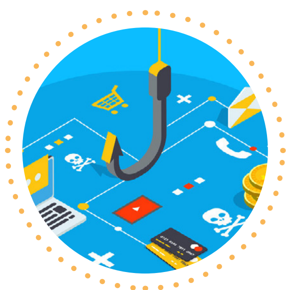
États-Nations

GÉOPOLITIQUE



Hacktivistes

IDÉOLOGIE



Cybercriminels

GAINS FINANCIERS



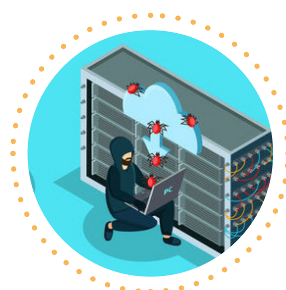
Groupes terroristes

VIOLENCE IDÉOLOGIQUE



Amateurs de sensations fortes

SATISFACTION



Menaces internes

MÉCONTENTEMENT

Dans le cyberespace, il faut se défendre non seulement contre les attaques directes, mais aussi contre les attaques globales



Mais la lecture est rarement aussi binaire et les intérêts s'imbriquent souvent. Un Etat pourrait très bien utiliser ses capacités pour espionner une entreprise ou une industrie dans un pays tiers afin d'en faire profiter sa propre industrie concurrente. Une société mal intentionnée pourrait désorganiser sa rivale en faisant appel à des cybercriminels.

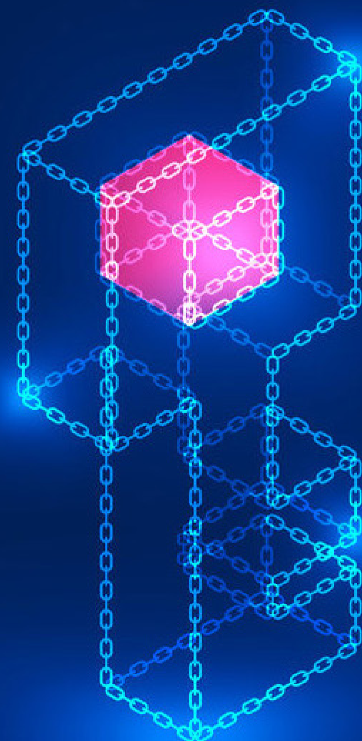
Des individus influents pourraient utiliser leur richesse pour orienter des scrutins afin de préserver leurs intérêts ou ceux de leurs pairs. Toute ressemblance avec des situations existant ou ayant existé… vous connaissez la suite.

Il peut paraître étrange de mélanger ainsi Etats, organisations criminelles ou génie solitaire de l'informatique. Mais c'est l'une caractéristique du cyberespace dont nous avons déjà parlé : l'affrontement devient asymétrique. **Un acteur isolé peut disposer d'une capacité de nuisance suffisante pour faire vaciller une grande organisation.**

Avant l'avènement des réseaux et du numérique, une telle situation était extrêmement rare. Ce n'est plus le cas.

En 2019, l'image romantique du pirate forçant les sécurités informatiques pour la beauté du geste a du plomb dans l'aile. Il en existe toujours, mais ils sont nettement moins nombreux que ceux qui sont animés par l'appât du gain. Le pirate peut aussi être mû par l'idéologie, qui l'amène à s'attaquer à des entités dont il ne partage pas les idées ou les actes.

Le "collectif" très médiatisé Anonymous en fait partie. Le piratage destiné au vol de données, à des fins politiques ou économiques, est également une menace répandue, qui peut émaner d'Etats comme d'autres organisations. Un pirate peut aussi chercher à nuire à sa victime à des degrés divers, d'une atteinte à sa réputation jusqu'à la destruction de ses données.



Si l'on se place du côté du chef d'entreprise, la menace ultime est toujours financière. Mais il y a un gouffre entre se faire ponctionner 1000 EUR par une opération d'hameçonnage par email frauduleux et se retrouver avec un outil de production à l'arrêt parce qu'il a fallu désactiver l'ERP.

Dans l'industrie, les enquêtes menées par les firmes spécialisées dans la sécurité informatique montrent que les dirigeants redoutent d'abord la paralysie de leur système d'information, ensuite des altérations de bases de données et enfin l'espionnage numérique.

Pour reprendre le cas NotPetya, l'attaque avait tout d'un "rançongiciel", c'est-à-dire un logiciel malveillant qui crypte des données et propose la clef de déchiffrement en échange d'un paiement. Sauf que les rares organisations qui ont payé la rançon n'ont jamais reçu de clef.

NotPetya a manifestement été conçu pour détruire définitivement des données, ce qui a provoqué de très gros dégâts chez des mastodontes comme Merck, TNT Express, Renault, Saint Gobain ou, nous l'avons déjà vu, chez Maersk.

La Maison Blanche a estimé le coût global de l'attaque à 10 milliards de dollars. Si une grande entreprise a d'importantes capacités de réaction, ce n'est pas le cas des plus petites. Une attaque du type de NotPetya peut ruiner une PME mal préparée.

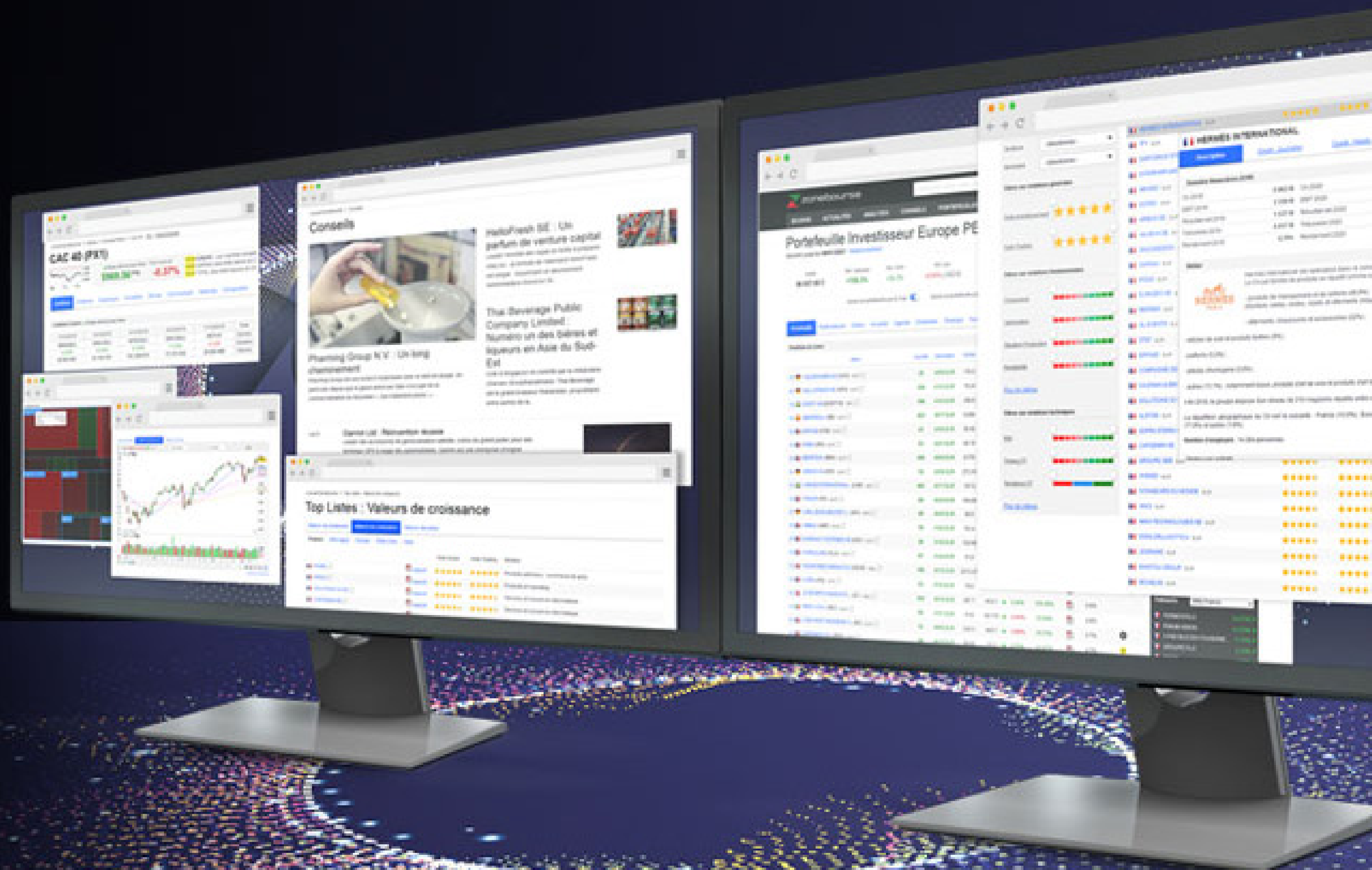
Il est important de rappeler que dans le cyberespace, il faut se défendre non seulement contre les attaques directes, mais aussi contre les attaques globales : Maersk n'était pas spécialement visé par NotPetya, mais le Danois en fut l'une des principales victimes.

zonebourse.com

Découvrez nos Solutions & Outils pour Investisseurs

Optimisez la performance de vos investissements dès maintenant.
Tous les outils, tous les conseils en un seul abonnement.

Découvrir



Les Moyens et les Enjeux



Les menaces qui pèsent sur une entreprise

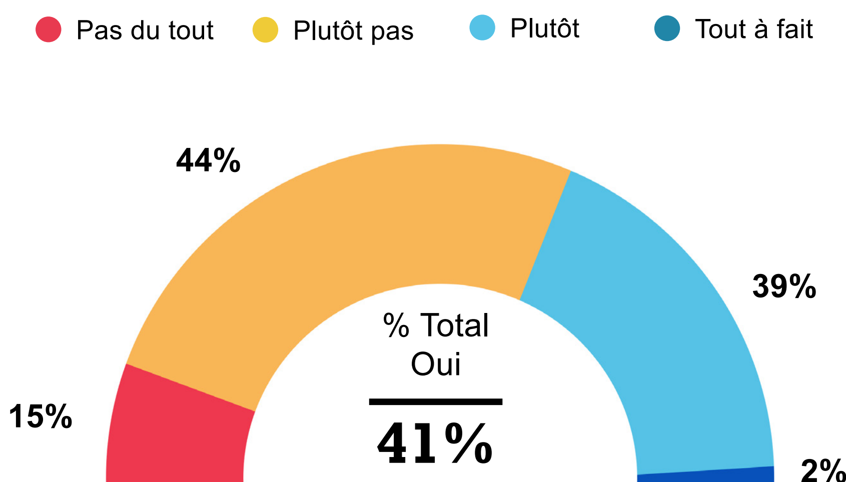
Les attaques contre les entreprises ne cessent de croître, nous avons vu pourquoi. **Toutefois, les systèmes de défense mis en place sont à même de parer la plupart d'entre elles en permanence**.

Mais ce qui inquiète tous les RSSI (responsable de la sécurité des systèmes d'information), c'est le "Big One", la cyberattaque d'envergure capable de déstabiliser momentanément l'entreprise.

Dans une enquête de janvier 2019 d'OpinionWay pour le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique), 59% des entreprises interrogées estiment qu'elles ne sont "pas du tout" ou "plutôt pas" préparées à une cyberattaque de grande ampleur. Le sondage a été réalisé à partir de 174 réponses d'adhérents du CESIN, soit des acteurs qui se préoccupent, a priori, davantage de cybersécurité que la moyenne.

Une enquête PwC d'octobre 2018 sur un panel plus large d'entreprises françaises conclut que 60% d'entre elles s'estiment en mesure de gérer une attaque (sans notion de grande ampleur). Dans ce même sondage, les entreprises ont aussi détaillé le type d'attaques dont elles ont fait l'objet. Comme le montre le tableau page 20, près des trois-quarts ont subi des tentatives d'hameçonnage, et la moitié des tentatives d'arnaque au président.

Votre entreprise est-elle préparée à gérer une cyber-attaque de grande ampleur ?



Source CESIN

“

Chaque grande ou moyenne entreprise déploie en moyenne 14 systèmes de défense



En moyenne, les sociétés qui ont répondu ont été confrontées à cinq types d'attaques différentes. Pour les contrer, elles déploient un arsenal impressionnant, qui explique l'essor des dépenses de cybersécurité.

En dehors des antivirus et firewall réglementaires, les entreprises disposent de 11,6 dispositifs de sécurité en moyenne ! Cela va d'un outil de gestion des accès à un système anti-attaque par déni de service, en passant par une passerelle VPN, du chiffrement ou une solution de gestion des logs. Cette accumulation de barrières doit permettre d'empêcher à un individu de se retrouver dans un périmètre qui lui est normalement interdit ou de comprendre comment il est entré.

Voyons maintenant quelques techniques d'intrusion, pour continuer à nous familiariser avec la cybersécurité.

Les entreprises doivent multiplier les outils pour protéger leurs réseaux, leurs systèmes et leurs données. Plusieurs fournisseurs sont souvent requis sur ce vaste marché.



Barbarians at the Gate

Les autorités françaises classent les "risques cyber" en quatre catégories : la cybercriminalité, l'atteinte à l'image, l'espionnage et le sabotage. Nous avons choisi de citer quelques exemples concrets, sans présenter de manière exhaustive toutes les possibilités d'intrusion.

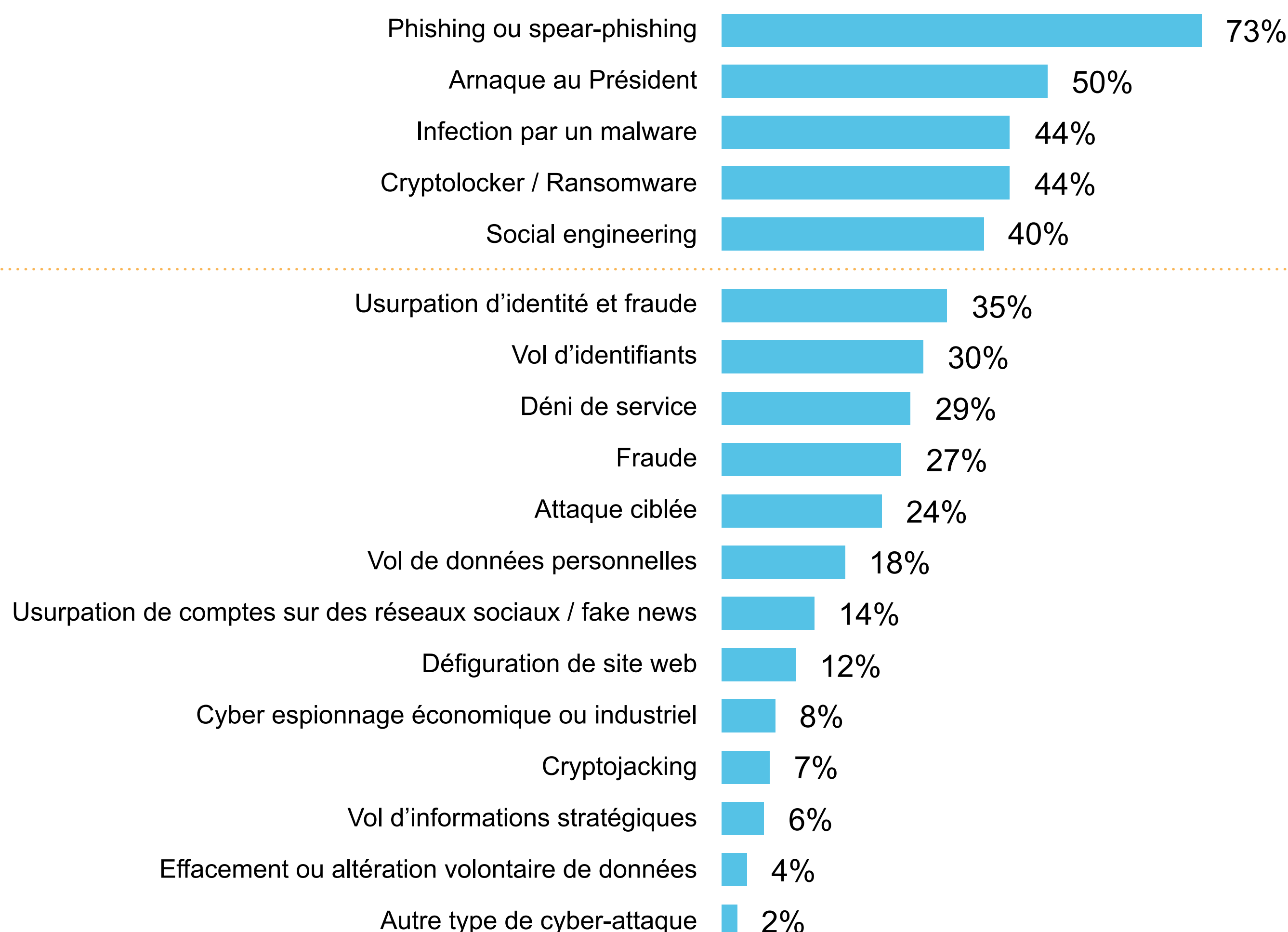


Souvenez-vous juste que la plupart du temps, une menace, pour être mise en œuvre, passe par la prise de contrôle d'un système informatique, donc par sa compromission d'une façon ou d'une autre.

Quel(s) type(s) de cyber-attaque votre entreprise a-t-elle constaté(s) au cours des 12 derniers mois ?

Base : ont constaté une attaque (139 répondants) / Plusieurs réponses possibles





Source CESIN

La cybercriminalité

La cybercriminalité a pour objectif d'obtenir des informations personnelles pour les exploiter de façon frauduleuse, soit en les utilisant directement soit en les mettant en vente pour des tiers dont les intentions ne sont pas plus amicales.

Nous l'avons vu quelques lignes plus haut, le mal le plus répandu est **l'hameçonnage (ou phishing)**. Un pirate achète une liste d'adresses de courriels sur le Dark Web, une partie du web non référencée par les moteurs habituels et accessible uniquement via des outils spécifiques quoique peu difficiles à mettre en œuvre.



Puis il prépare un message destiné à berner le destinataire pour récupérer des données le concernant en se faisant passer pour un "tiers de confiance". Les attaques basiques jouent sur la masse pour pêcher quelques poissons et leur soutirer, par exemple, leurs codes de carte bancaire. Si le pirate dispose d'une base de données un peu plus sophistiquée, c'est-à-dire comprenant déjà des éléments personnels sur les propriétaires de courriels, il pourra encore mieux maquiller son hameçonnage.

Un exemple ? Les hôtels Marriott ont révélé il y a quelques mois que leur système de réservation avait été compromis et que les données de leurs clients avaient été dérobées. Noms, adresses, numéros de téléphone, dates de séjour et numéros de passeport de 327 millions de personnes sont partis dans la nature, dont une partie non-cryptée. **Il faut bien comprendre qu'une fois qu'un courriel a été corrompu, il est en vente ad vitam aeternam sur le Dark Web.**

Quand les pirates disposent d'informations additionnelles, les bibliothèques des cybercriminels s'enrichissent. Plus ils en savent sur un individu, plus ils pourront cibler leurs offensives. Si Monsieur A est identifié comme un haut dirigeant d'entreprise séjournant régulièrement à New York et ayant pour numéro de passeport X et de téléphone Y, il sera bien plus facile de concevoir un courriel malveillant pour monter une extorsion de fonds crédible.

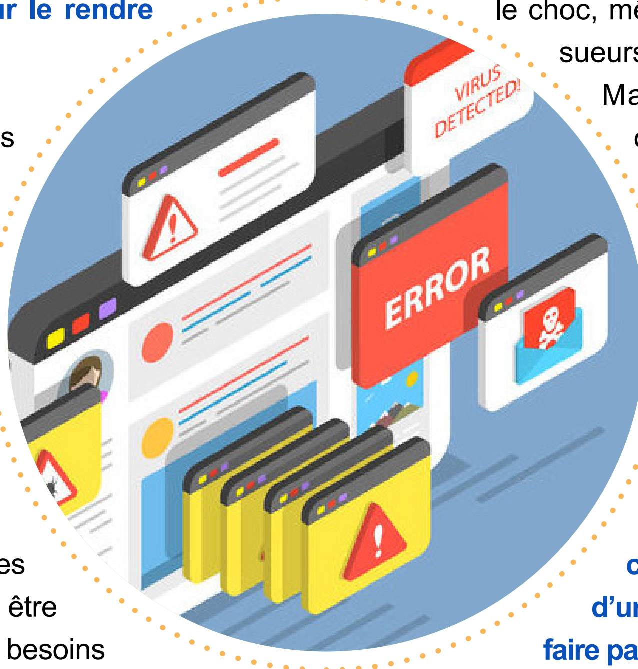
On parle ici d'ingénierie sociale : c'est la capacité du cybercriminel à exploiter ce qu'il sait sur sa victime pour mieux le berner.

L'autre version très connue du cybercrime est le rançongiciel (ransomware). Le pirate introduit un outil (maliciel, ou malware en anglais) sur une machine, qui bloque l'accès à des données et demande à la victime de payer une somme (le plus souvent en cryptomonnaie) pour obtenir la clef de déchiffrement. Le maliciel est généralement contenu dans un courriel (quatre fois sur cinq environ) et requiert une intervention humaine : cliquer sur un lien ou ouvrir une pièce jointe. Certains maliciels particulièrement vicieux peuvent aussi se télécharger à l'insu de l'utilisateur, par exemple via un navigateur qui n'est plus mis à jour. Cybersecurity Ventures estime que les rançongiciels coûteront au global 11,5 milliards de dollars en 2019. Ce montant cumule les sommes obtenues par les cybercriminels, les coûts de désorganisation et les frais de lutte.

L'atteinte à l'image

L'atteinte à l'image est destinée à déstabiliser une structure, le plus souvent une entreprise, une administration ou une organisation tierce.

Largement médiatisées, les attaques par déni de service (souvent nommées par leur acronyme anglo-saxon DoS) consistent à saturer un site ou un service internet pour le rendre indisponible.



Grâce au développement des réseaux, les pirates sont en mesure de décupler la puissance de saturation en faisant appel à une multitude d'équipements connectés (on parle alors de DDoS, attaque par déni de service distribuée).

Il s'agit de machines infectées par des virus qui peuvent être activées ensemble pour les besoins d'une attaque. Dans le jargon, ce dispositif est qualifié de "réseau zombie" ou plus souvent de "botnet". Ils sont la plupart du temps dormants. Certains sont proposés à la location aux individus malintentionnés. Une sorte de "Botnet-as-a-Service".

En 2016, l'hébergeur européen OVH avait subi une violente attaque DDoS (la plus sévère de l'histoire à l'époque). Son originalité est qu'elle s'appuyait sur un réseau de botnets constitué majoritairement d'objets internet connectés, en particuliers des caméras bas de gamme.

L'avantage de ces matériels, du moins pour un attaquant, est qu'ils sont nombreux, connectés en permanence à Internet, qu'ils convoient de la vidéo (donc de gros volumes de données) et qu'ils sont faiblement protégés (les mots de passe constructeurs sont rarement modifiés). Lors du raid sur OVH, ou plutôt sur de gros clients de l'hébergeur, tout le réseau de botnets a été dirigé sur les serveurs pour les mettre hors service.

Malgré l'ampleur de l'attaque, l'infrastructure a tenu le choc, même si elle a donné quelques sueurs froides aux défenseurs. Mais la multiplication des objets connectés entraînera inévitablement de nouveaux risques. A quand une attaque DDoS de réfrigérateurs ?

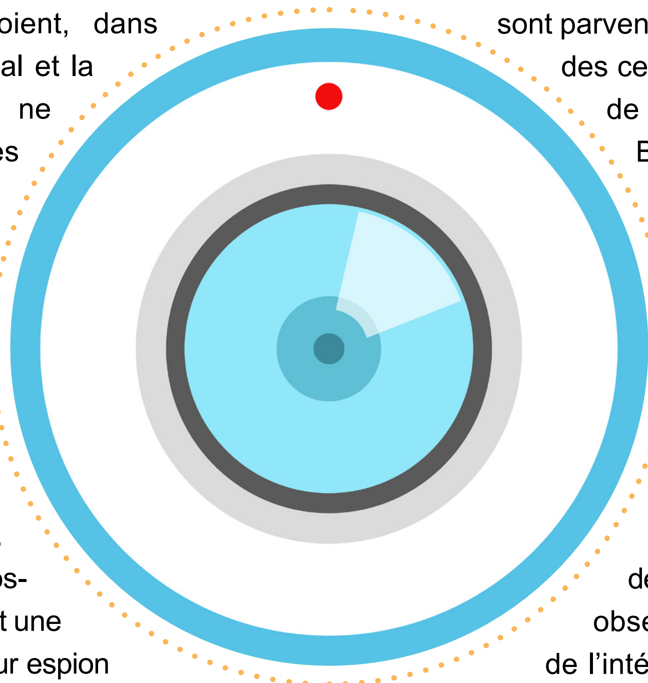
L'autre attaque-type d'atteinte à l'image citée par les autorités françaises est la défiguration (defacement pour les anglo-saxons), qui consiste à modifier l'aspect d'un site internet ou intranet pour faire passer un message.

La plupart du temps, il s'agit pour des pirates de faire passer un message idéologique en modifiant le site internet d'une organisation dont ils ne partagent pas les actions ou les idées.

Cela peut aussi prendre un tour plus léger, comme en 2009 lorsqu'un plaisantin avait remplacé la photo de José-Luis Zapatero par celle de Mr. Bean sur le site de la présidence espagnole de l'Europe. Mais il est aussi possible par ce biais d'opérer des malversations plus sophistiquées, par exemple en vue de récupérer des données personnelles.

L'espionnage

Le développement du stockage numérique et l'exploitation des données est à la fois une bénédiction et une source d'inquiétude pour les organisations. L'accès à la connaissance d'autrui (l'ennemi, le concurrent, le tiers) a toujours constitué un atout considérable. Il n'est donc pas étonnant que les secteurs industriels les plus visés par l'espionnage soient, dans l'ordre, l'armement, le spatial et la santé. Les administrations ne sont pas en reste puisque les exemples de piratage sont nombreux, dans tous les pays.



Par rapport à un hameçonnage ou à une attaque par déni de service, l'espionnage informatique est une spécialité plus raffinée. Pour être le plus efficace possible, il réclame de l'habilité et une bonne préparation. Le meilleur espion n'est-il pas celui qui se fond dans le décor et qui sort des informations pendant le temps le plus long possible ? A moins que ce ne soit celui qui a éliminé toute trace de son passage ? Dans un cas comme dans l'autre, il s'agit d'infiltrer une structure sans qu'elle se soit rendue compte d'une quelconque présence.

Un Etat pourra chercher à connaître les intentions d'un autre pour des raisons géopolitiques. En France, le piratage du ministère des finances en 2011 (150 postes compromis) est souvent cité en exemple comme un espionnage politique, en amont de l'organisation du G20 dans l'hexagone. Mais puisqu'on en parle, c'est qu'il a été découvert et qu'il n'a par conséquent pas eu l'effet maximum escompté.

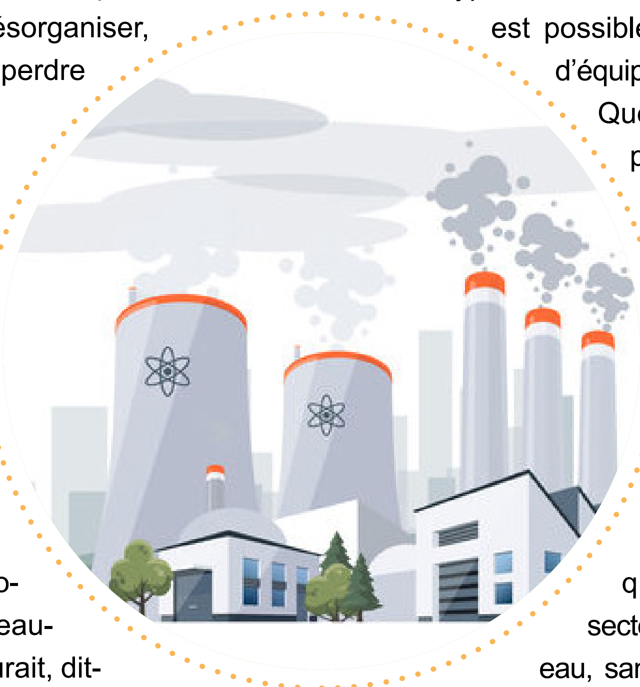
A la frontière entre deux risques cyber, des pirates sont parvenus à faire émettre à leur profit des centaines de millions de dollars de virements de la Banque du Bangladesh en 2017.

Si la plupart ont pu être bloqués grâce à la vigilance d'une banque tierce, 81 millions de dollars se sont évanouis dans la nature. Par quel moyen ? Après avoir réussi à introduire un logiciel espion dans le réseau de la banque, ils ont patiemment observé pendant plusieurs mois, de l'intérieur, les processus internes jusqu'à identifier une méthode valable pour leur larcin.

Des techniques d'espionnage ont conduit à une opération de cybercriminalité d'ampleur, qui figure au palmarès des plus gros braquages numériques de l'histoire.

Le sabotage

Quand nous évoquions précédemment le "Big One" tant redouté par les entreprises et les administrations françaises, c'est de sabotage dont il est question. Cette catégorie de menace est de loin celle qui a les conséquences les plus graves. Dans ce scénario, l'assaillant cherche à faire des dégâts à l'infrastructure d'une entreprise ou d'une administration, pour la désorganiser, l'endommager ou lui faire perdre des données.



Commençons par un exemple célèbre. Stuxnet est un maliciel (malware) découvert en 2010, qui a été développé pour se frayer un chemin, via des failles de sécurité, jusque dans le SCADA (système de pilotage d'installations techniques) de certains produits Siemens. Le ver a beaucoup fait parler de lui car il aurait, dit-on, permis de retarder le développement du programme nucléaire iranien. Schématiquement, Stuxnet a permis d'altérer le fonctionnement normal des centrifugeuses d'enrichissement d'uranium du site de Natanz pour accélérer leur usure et dégrader la qualité de leur production. En toute discrétion. Le maliciel a été attribué aux Etats-Unis et à Israël, bien que rien ne permette de l'affirmer avec certitude.

Ce type d'attaque est très sophistiqué. Le développement du maliciel a pris du temps, il a fallu l'introduire dans l'infrastructure en mode Cheval de Troie, attendre qu'il parvienne jusqu'à un poste équipé du logiciel adéquat puis qu'il entre en action suffisamment longtemps, sans se faire repérer donc, pour mener à bien son dessein. Stuxnet semblait viser spécifiquement un Etat, ce qui ne l'a pas empêché de réapparaître ailleurs et d'infecter d'autres équipements Siemens dans le monde, notamment en France. Une véritable cyberarme, aux dires des spécialistes, particulièrement inquiétante au regard de son degré de sophistication. D'autres maliciels de ce type sont en circulation. Ils démontrent qu'il est possible d'altérer le fonctionnement d'équipements importants à distance. Que se passerait-il si un pirate prenait le contrôle d'une centrale nucléaire ou d'un aéroport ?

Ce type de scénario donne des sueurs froides aux autorités de tous les pays de la planète. En France, l'Etat a défini des "OIV", ou "opérateurs d'importance vitale", qui opèrent dans plusieurs secteurs stratégiques (alimentation, eau, santé, activités de l'Etat, énergie, transport, finance, communications, audiovisuel, industrie, espace & recherche). Ces 249 acteurs ont des obligations strictes en matière de cybersécurité, aussi bien en protection qu'en plans de réaction. Leur liste complète n'est pas publique mais on y retrouve par exemple EDF pour l'énergie, Veolia pour l'eau, la SNCF pour le transport ou Orange pour les télécoms. Il existe aussi désormais des "OSE" (opérateurs de services essentiels) et "FSN" (fournisseurs de services numériques), assujettis eux aussi à certaines obligations sécuritaires.

Le patron de l'Anssi, Guillaume Poupard, ne fait pas de mystère quant à sa préoccupation principale : l'attaque de sabotage d'une infrastructure, par un Etat ou à des fins terroristes, figure tout en haut de la liste.

Conclusion

Une grosse attaque informatique a la vertu de déclencher chez l'organisation victime une véritable prise de conscience de sa vulnérabilité. Le reste du temps, il faut bien dire que les RSSI ont du mal à convaincre leurs conseils d'administration d'aller aussi loin qu'ils le souhaiteraient, eux qui savent pertinemment que le diable se cache dans les détails. Dans notre exemple précité, les dirigeants de Maersk ont changé leur fusil d'épaule pour éviter de revivre les jours maudits de juin 2017.

Les équipes IT avaient dû, en quelques jours, réinstaller 4 000 serveurs, fournir quatre fois plus d'ordinateurs vierges aux employés et redéployer tous les logiciels nécessaires. Il y a un an à Davos, le président du Danois avait loué la rapidité avec laquelle ses équipes avaient redressé la barre. "Nous étions très moyens en matière de cybersécurité, comme la plupart des autres entreprises", a-t-il concédé…

Désormais, Maersk a élevé sa politique de sécurité informatique au niveau des meilleurs standards, jusqu'à en faire un argument commercial.

Chez Saint-Gobain, les retombées de NotPetya n'ont pas été aussi dramatiques. Mais elles furent coûteuses malgré tout et ont fait office d'électrochoc. La cybersécurité est devenue au sein de l'entreprise tricentenaire un "sujet de priorité absolue", qui l'a conduite à monter un véritable plan de cyberdéfense et à mettre à niveau sa politique et ses outils de lutte, notamment à travers des formations obligatoires et l'introduction de solutions innovantes comme les "bacs à sable" ("sandbox", environnements sécurisés qui permettent de tester des contenus suspects) et l'intelligence artificielle (pour identifier les anomalies plus rapidement).

Les pages qui précèdent, en plus de dresser un rapide état des lieux des menaces, montrent que le marché de la cybersécurité a de beaux jours devant lui. Passons au second volet de notre décryptage grand angle, pour identifier les entreprises qui proposent des outils et des prestations de protection, avant de présenter une sélection d'acteurs cotés européens qui vont bénéficier de la croissance continue des besoins.

NOTRE SÉLECTION DE VALEURS

Complément indispensable de l'investisseur avisé, cette liste vous fournit une sélection de valeurs exposées à la thématique cybersécurité, pour vous permettre d'identifier les perles rares d'un secteur incontournable de l'ère numérique. Le marché de la sécurité informatique pourrait avoisiner les 300 milliards de dollars par an en 2024. Prêt à découvrir qui va en profiter ?

Accédez à notre
Liste Thématique Cybersécurité

Découvrir



© Zonebourse.com 2019
Les analyses réalisées par SURPERFORMANCE SAS, société éditrice du site Zonebourse.com, n'ont aucune valeur contractuelle et ne constituent en aucun cas une offre de vente ou une sollicitation d'achat de produits ou services financiers. SURPERFORMANCE SAS décline toute responsabilité dans l'utilisation qui pourrait être faite des informations qu'elle diffuse et des conséquences qui pourraient en découler, notamment de toute décision prise sur la base des informations contenues sur le Site, y compris en cas d'erreur ou d'omission. Les informations, graphiques, chiffres, opinons ou commentaires rédigés par les équipes de rédaction de SURPERFORMANCE SAS ou mis à disposition par cette dernière s'adressent à des investisseurs disposant des connaissances et expériences nécessaires pour comprendre et apprécier les informations qui y sont développées. Ces dernières sont diffusées à titre purement indicatif. SURPERFORMANCE SAS ne peut en garantir l'exactitude ou la fiabilité. L'intégralité des textes, photographies, images, graphiques, logos, bases de données et toute autre forme de contenu de quelque nature qu'elle soit, est protégée au titre de la propriété intellectuelle. Toute reproduction, transmission ou rediffusion, même partielle, sous quelque forme que ce soit, est strictement interdite.